UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,301	11/02/2001	Bridget J. Frey	PLM007001	8153

29585 7590 03/22/2005

DLA PIPER RUDNICK GRAY CARY US LLP
153 TOWNSEND STREET
SUITE 800
SAN FRANCISCO, CA 94107-1907

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/004,301	FREY ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 November 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/20/03, 6/26/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 408 (page 4, line 1, perhaps 208 was intended), 306 (page 12, line 5, perhaps 506 was intended), 616 (page 14, line 3), 302, 304 (page 14, line 31), 734A (page 15, line 11). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities: "LDAP", "NT", "ODBC" (page 11, line 30), "EPROM", "EEPROM" (page 17, line 31). While well known in the art, these terms have not been defined.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11, 27, 43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 11, 27, 43 recite the limitation "wherein the Web resource includes a Web site" in line 1 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Wood et al. (US Patent Number: 6,668,322).

Regarding claim 1, Wood et al. teach receiving a signal representing a request from a remote user for a secure resource residing on a network employing a generic application-layer network protocol (column 9, lines 19-40); determining, without the intervention of the user, the type of security credential required to access the secure

resource (column 9, lines 65-67, column 10, lines 1-29); and sending a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 2, Wood et al. teach authenticating the user before sending the signal representing the second request (column 12, lines 10-37).

Regarding claim 3, Wood et al. teach further comprising: receiving a signal representing a response to the second request (column 15, lines 5-6); and sending a signal representing a result to the remote user (column 15, lines 7-8), the result based on the response to the second request (column 14, lines 60-67, column 15, lines 1-8).

Regarding claim 4, Wood et al. teach wherein the request includes a logon credential for the remote user, further comprising: authenticating the remote user based on the logon credential before sending the second request (column 14, lines 20-60).

Regarding claim 5, Wood et al. teach wherein the request includes a logon credential for the remote user and the type of security credential required to access the secure resource includes the logon credential, further comprising: sending the signal representing the second request to the secure resource, the second request including the logon credential (column 14, lines 20-67).

Regarding claim 6, Wood et al. teach wherein the request includes a logon credential for the remote user, further comprising: receiving a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential (column 13, lines 60-67, column 14, lines 1-10); and sending a signal

representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 7, Wood et al. teach sending a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token (column 6, lines 9-56).

Regarding claim 8, Wood et al. teach receiving a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential (column 13, lines 60-67, column 14, lines 1-10); and sending a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 9, Wood et al. teach wherein the generic application-layer network protocol is hypertext transfer protocol (column 9, lines 19-40, column 11, lines 1-11).

Regarding claim 10, Wood et al. teach receiving a signal representing data in response to the second request (column 15, lines 1-8); and sending a signal representing at least a portion of the data to the remote user (column 15, lines 1-8).

Regarding claim 11, Wood et al. teach wherein the Web resource includes a Web site, and the data is hypertext mark-up language (column 15, lines 1-8).

Regarding claim 12, Wood et al. teach wherein receiving includes receiving a signal representing a request from the remote user for a second secure resource residing on the network (column 9, lines 53-64), further comprising: determining, without the intervention of the user, the type of security credential required to access the second secure resource (column 9, lines 65-67, column 10, lines 1-29); and sending a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access the second secure resource (column 12, lines 66-67, column 13, lines 1-20); and wherein the signals representing the second and third requests are sent concurrently (column 9, lines 19-64).

Regarding claim 13, Wood et al. teach wherein the types of security credentials included in the second and third requests differ (column 16, lines 15-35).

Regarding claim 14, Wood et al. teach wherein the types of security credentials included in the second and third requests are the same (column 16, lines 15-35).

Regarding claim 15, Wood et al. teach receiving a signal representing the security credential from the user before receiving the signal representing the request (column 13, lines 30-37, column 14, lines 4-20).

Regarding claim 16, Wood et al. teach storing the security credential at least until sending the signal representing the second request (column 13, lines 30-37, column 14, lines 4-20).

Regarding claim 17, Wood et al. teach means for receiving a signal representing a request from a remote user for a secure resource residing on a network employing a

generic application-layer network protocol (column 9, lines 19-40); means for determining, without the intervention of the user, the type of security credential required to access the secure resource (column 9, lines 65-67, column 10, lines 1-29); and means for sending a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 18, Wood et al. teach means for authenticating the user before sending the signal representing the second request (column 12, lines 10-37).

Regarding claim 19, Wood et al. teach means for receiving a signal representing a response to the second request (column 15, lines 5-6); and means for sending a signal representing a result to the remote user (column 15, lines 7-8), the result based on the response to the second request (column 14, lines 60-67, column 15, lines 1-8).

Regarding claim 20, Wood et al. teach wherein the request includes a logon credential for the remote user, further comprising: means for authenticating the remote user based on the logon credential before sending the second request (column 14, lines 20-60).

Regarding claim 21, Wood et al. teach wherein the request includes a logon credential for the remote user and the type of security credential required to access the secure resource includes the logon credential, further comprising: means for sending the signal representing the second request to the secure resource, the second request including the logon credential (column 14, lines 20-67).

Regarding claim 22, Wood et al. teach wherein the request includes a logon credential for the remote user, further comprising: means for receiving a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential (column 13, lines 60-67, column 14, lines 1-10); and means for sending a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 23, Wood et al. teach means for sending a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token (column 6, lines 9-56).

Regarding claim 24, Wood et al. teach means for receiving a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential (column 13, lines 60-67, column 14, lines 1-10); and means for sending a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 25, Wood et al. teach wherein the generic application-layer network protocol is hypertext transfer protocol (column 9, lines 19-40, column 11, lines 1-11).

Regarding claim 26, Wood et al. teach means for receiving a signal representing data in response to the second request (column 15, lines 1-8); and means for sending a signal representing at least a portion of the data to the remote user (column 15, lines 1-8).

Regarding claim 27, Wood et al. teach wherein the Web resource includes a Web site, and the data is hypertext mark-up language (column 15, lines 1-8).

Regarding claim 28, Wood et al. teach wherein means for receiving includes means for receiving a signal representing a request from the remote user for a second secure resource residing on the network (column 9, lines 53-64), further comprising: means for determining, without the intervention of the user, the type of security credential required to access the second secure resource (column 9, lines 65-67, column 10, lines 1-29); and means for sending a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access the second secure resource (column 12, lines 66-67, column 13, lines 1-20); and wherein the signals representing the second and third requests are sent concurrently (column 9, lines 19-64).

Regarding claim 29, Wood et al. teach wherein the types of security credentials included in the second and third requests differ (column 16, lines 15-35).

Regarding claim 30, Wood et al. teach wherein the types of security credentials included in the second and third requests are the same (column 16, lines 15-35).

Regarding claim 31, Wood et al. teach means for receiving a signal representing the security credential from the user before receiving the signal representing the request (column 13, lines 30-37, column 14, lines 4-20).

Regarding claim 32, Wood et al. teach means for storing the security credential at least until sending the signal representing the second request (column 13, lines 30-37, column 14, lines 4-20).

Regarding claim 33, Wood et al. teach receiving a signal representing a request from a remote user for a secure resource residing on a network employing a generic application-layer network protocol (column 9, lines 19-40); determining, without the intervention of the user, the type of security credential required to access the secure resource (column 9, lines 65-67, column 10, lines 1-29); and sending a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 34, Wood et al. teach wherein the method further comprises: authenticating the user before sending the signal representing the second request (column 12, lines 10-37).

Regarding claim 35, Wood et al. teach wherein the method further comprises: receiving a signal representing a response to the second request (column 15, lines 5-6); and sending a signal representing a result to the remote user (column 15, lines 7-8), the result based on the response to the second request (column 14, lines 60-67, column 15, lines 1-8).

Regarding claim 36, Wood et al. teach wherein the request includes a logon credential for the remote user, wherein the method further comprises: authenticating the remote user based on the logon credential before sending the second request (column 14, lines 20-60).

Regarding claim 37, Wood et al. teach wherein the request includes a logon credential for the remote user and the type of security credential required to access the secure resource includes the logon credential, wherein the method further comprises: sending the signal representing the second request to the secure resource, the second request including the logon credential (column 14, lines 20-67).

Regarding claim 38, Wood et al. teach wherein the request includes a logon credential for the remote user, wherein the method further comprises: receiving a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential (column 13, lines 60-67, column 14, lines 1-10); and sending a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 39, Wood et al. teach wherein the method further comprises: sending a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token (column 6, lines 9-56).

Regarding claim 40, Wood et al. teach wherein the method further comprises: receiving a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential (column 13, lines 60-67, column 14, lines 1-10); and sending a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential (column 12, lines 66-67, column 13, lines 1-20).

Regarding claim 41, Wood et al. teach wherein the generic application-layer network protocol is hypertext transfer protocol (column 9, lines 19-40, column 11, lines 1-11).

Regarding claim 42, Wood et al. teach wherein the method further comprises: receiving a signal representing data in response to the second request (column 15, lines 1-8); and sending a signal representing at least a portion of the data to the remote user (column 15, lines 1-8).

Regarding claim 43, Wood et al. teach wherein the Web resource includes a Web site, and the data is hypertext mark-up language (column 15, lines 1-8).

Regarding claim 44, Wood et al. teach wherein receiving includes receiving a signal representing a request from the remote user for a second secure resource residing on the network (column 9, lines 53-64), wherein the method further comprises: determining, without the intervention of the user, the type of security credential required to access the second secure resource (column 9, lines 65-67, column 10, lines 1-29); and sending a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access

the second secure resource (column 12, lines 66-67, column 13, lines 1-20); and wherein the signals representing the second and third requests are sent concurrently (column 9, lines 19-64).

Regarding claim 45, Wood et al. teach wherein the types of security credentials included in the second and third requests differ (column 16, lines 15-35).

Regarding claim 46, Wood et al. teach wherein the types of security credentials included in the second and third requests are the same (column 16, lines 15-35).

Regarding claim 47, Wood et al. teach wherein the method further comprises: receiving a signal representing the security credential from the user before receiving the signal representing the request (column 13, lines 30-37, column 14, lines 4-20).

Regarding claim 48, Wood et al. teach wherein the method further comprises: storing the security credential at least until sending the signal representing the second request (column 13, lines 30-37, column 14, lines 4-20).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100